CLAIMS

What is claimed is:

1. A method for a provider of software to authenticate users of the software, comprising the steps of:

constructing a puzzle in response to information received from a user, the puzzle including the information;

sending the puzzle to the user; and

returning a solution to the puzzle to the provider.

2. The method of claim 1, wherein the information comprises demographic information about the user.

3. The method of claim 1, wherein the information comprises an identity of the user.

4. The method of claim 1, wherein the constructing step comprises the steps of deriving a value from the information to produce a derived value, exponentiating the derived value to produce an exponentiated value, and combining the exponentiated value with a portion of the derived value.

5. The method of claim 4, further comprising the steps of storing the information and a random number, performing a hash function on the information and the random number to generate a first hash result, and encrypting the first hash result, wherein the deriving step comprises the steps of partitioning the encrypted hash result into first and second components, performing a hash function on a concatenation of the first component and the random number to generate a second hash result, appending a plurality of zero values to the second component to produce a lengthened second component, performing an exclusive-OR operation between the lengthened second component and the second hash

result to generate an exclusive-OR result, and concatenating the first component and the exclusive-OR result to produce the value.

6. The method of claim 4, wherein the exponentiating step comprises the steps of raising a generator to a power, the power being the derived value, dividing the generator raised to the power of the derived value by a prime number, and obtaining the remainder of the division operation.

7. An apparatus for enabling a provider of software to authenticate users of the software, comprising:

means for constructing a puzzle in response to information received from a user, the puzzle including the information;

means for sending the puzzle to the user; and

means for returning a solution to the puzzle to the provider.

8. The apparatus of claim 7, wherein the information comprises demographic information about the user.

9. The apparatus of claim 7, wherein the information comprises an identity of the user.

10. The apparatus of claim 7, wherein the means for constructing a puzzle comprises means for deriving a value from the information to produce a derived value, means for exponentiating the derived value to produce an exponentiated value, and means for combining the exponentiated value with a portion of the derived value.

11. The apparatus of claim 10, further comprising means for storing the information and a random number, means for performing a hash function on the information and the random number to generate a first hash result, and means for encrypting the first hash result, wherein the means for deriving means for partitioning the encrypted hash result into first and second components,

performing a hash function on a concatenation of the first component and the random number to generate a second hash result, appending a plurality of zero values to the second component to produce a lengthened second component, performing an exclusive-OR operation between the lengthened second component and the second hash result to generate an exclusive-OR result, and concatenating the first component and the exclusive-OR result to produce the value.

12. The apparatus of claim 10, wherein the means for exponentiating comprises means for raising a generator to a power, the power being the derived value, means for dividing the generator raised to the power of the derived value by a prime number, and means for obtaining the remainder of the division operation.

13. An apparatus for enabling a provider of software to authenticate users of the software, comprising:

a processor; and

a processor-readable storage medium accessible by the processor and containing a set of instructions executable by the processor to construct a puzzle in response to information received from a user, the puzzle including the information, and send the puzzle to the user.

14. The apparatus of claim 13, wherein the information comprises demographic information about the user.

15. The apparatus of claim 13, wherein the information comprises an identity of the user.

16. The apparatus of claim 13, wherein the puzzle is constructed by deriving a value from the information to produce a derived value, exponentiating the derived value to produce an exponentiated value, and combining the exponentiated value with a portion of the derived value.

17. The apparatus of claim 16, wherein the set of instructions is further executable by the processor to store the information and a random number, perform a hash function on the information and the random number to generate a first hash result, and encrypt the first hash result, wherein the derived value is derived by partitioning the encrypted hash result into first and second components, performing a hash function on a concatenation of the first component and the random number to generate a second hash result, appending a plurality of zero values to the second component to produce a lengthened second component, performing an exclusive-OR operation between the lengthened second component and the second hash result to generate an exclusive-OR result, and concatenating the first component and the exclusive-OR result to produce the value.

18. The apparatus of claim 16, wherein the exponentiated value is exponentiated by raising a generator to a power, the power being the derived value, dividing the generator raised to the power of the derived value by a prime number, and obtaining the remainder of the division operation.

19. A method of preventing a person from impersonating a plurality of users of software, comprising the steps of:

constructing a plurality of puzzles, each puzzle having a solution that includes information about a respective one of the plurality of users, each puzzle requiring consumption of a resource to solve; and

sending each puzzle to a respective one of the plurality of users for solution.

20. The method of claim 19, wherein the resource is computer processing time.